UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /aba	8250

7380 7590 11/16/2006

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 11/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/702,540	SO, VINCENT	
	Examiner	Art Unit	
	Charlie C. Agwumezie	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/7/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 15, 24, 25, 26, 27, 28, 29, 30, 31, 32 and 38, are rejected under 35 U.S.C. 102(e) as being anticipated by Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1.

1. As per **claims 1, 15 and 38**, Peterka et al discloses a method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections (0080; 0082; 0101);

delivering the plurality of encrypted sections to the customer processing platform (fig. 8; 0080; 0082); and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are

delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (0080; 0082; 0102; ...client has possession of program segment key and next the key...).

24. As per **claim 24**, Peterka et al discloses a method of ordering data content for delivery over a communication network, comprising:

displaying product or service information associated with a service provider at a customer interface of an interactive device accessible to a customer (fig. 6; 0073; 0086);

registering the customer with the service provider (0046; 0047; 0055; 0140);

transmitting customer verification information and order information requesting data content, input by the customer using the customer interface, to the service provider (0055);

comparing the customer verification information with corresponding customer verification information accessible to the service provider (0055; 0072; 0140); and

where the customer verification information matches the corresponding customer verification information accessible to the service provider:

segregating the requested data content into a plurality of sections (0080; 0082);

encrypting each section of the data content with a respective encryption key (0080; 0082);

delivering the encrypted data content to the interactive device (fig. 9); and

billing an account of the customer (figs. 8 and 9).

25. As per **claim 25**, Peterka et al further discloses the method, wherein registering comprises receiving input of customer identification information on a network registration transmitting device and transmitting the customer identification information to the service provider (0072; 0073).

26. As per **claim 26**, Peterka et al further discloses the method, wherein the customer identification information comprises network address information (0072; 0123).

27. As per **claim 27**, Peterka et al further discloses the method, wherein the customer verification information accessible to the service provider comprises the customer identification information (0072; 0123).

28. As per **claim 28**, Peterka et al further discloses the method, wherein the customer verification information transmitted to the service provider comprises network address information and a customer identification number (0072; 0123).

29. As per **claim 29**, Peterka et al further discloses the method, further comprising:

confirming delivery of the encrypted data content to the interactive device, wherein billing of the account of the customer is responsive to confirming delivery of the encrypted data content (figs. 8, 9 and 12; 0115; 0140).

30. As per **claim 30**, Peterka et al further discloses the method, wherein the segregating and encrypting were previously performed, wherein the encrypted data content is stored at the service provider, and wherein the stored encrypted content is retrieved and delivered to the interactive device where the customer verification information matches the corresponding customer verification information accessible to the service provider (0064; 0074).

31. As per **claim 31**, Peterka et al further discloses the method, wherein the data content is received by the service provider from a data content provider (fig. 1).

32. As per **claim 32**, Peterka et al further discloses the method, wherein the encrypted data content is obtained by the service provider from a data content provider and delivered to the interactive device where the customer verification information matches the corresponding customer verification information accessible to the service provider (fig. 1; 0064; 0074).

Claims 35, 36 and 37, are rejected under 35 U.S.C. 102(e) as being anticipated by Mourad et al U.S. Patent Application Publication No. 2006/0053077 A1.

35. As per **claims 35, and 37**, Mourad et al discloses a computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading data content to a customer computer system from a data content service provider system or another customer computer system (fig. 14 and 16; 0018; 0169; 0171; 0212); and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system (0251; 0255).

36. As per **claim 36**, Mourad et al further discloses the computer readable medium, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content (0251).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-13, 16-19, 21-23, 39, and 40-42, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Stirling et al U.S. patent Application Publication No. 2003/0223583 A1.

2. As per **claim 2**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a first key of the plurality of decryption keys for a first encrypted section of the plurality of encrypted sections (figs. 3 and 6; 0080; 0082);

delivering to the customer processing platform a second key of the plurality of decryption keys for a second encrypted section of the plurality of encrypted sections (0007).

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Stirling et al discloses the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

3. As per **claim 3**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys for a current encrypted section of the plurality of encrypted sections to be processed at the customer processing platform (0080; 0082);

delivering to the customer processing platform a next key of the plurality of decryption keys for a next encrypted section of the plurality of encrypted sections to be subsequently processed at the customer processing platform upon completion of processing of the current encrypted section (0080; 0082; 0102; ...client has possession of program segment key and next key...).

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Stirling et al discloses method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

4. As per **claim 4**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082) and

What Peterka does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

Stirling et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

5. As per **claim 5**, Peterka et al discloses the method, wherein the current encrypted section is a first one of the plurality of encrypted sections (0080; 0082), and wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082).

What Peterka et al does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

Stirling et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

6. As per **claim 6**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to: receive a decryption key for one of the plurality of encrypted sections (0080; 0082; 0117; 0118);

complete decryption of the one section (0080; 0082).

What Peterka et al does not explicitlt teach is

destroy the decryption key.

Stirling et al discloses a method comprising destroy the decryption key (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the

method of destroy the decryption key in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

7. As per **claim 7**, Peterka et al further discloses the method further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform (figs. 8 and 9).

8. As per **claim 8**, Peterka et al further discloses the method, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content (0033; 0080; 0082).

9. As per **claim 9**, Peterka et al further discloses the method, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key (0080; 0082; 0117).

10. As per **claim 10**, Peterka et al further discloses the method, further comprising:

generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys (0097; 0114; 0124).

11. As per **claim 11**, Peterka et al further discloses the method, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value (0097; 0114; 0124; claim 23).

12. As per **claim 12**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values (0097; 0114; 0124; claim 23).

13. As per **claim 13**, Peterka et al further discloses the method, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform (0097; 0114; 0124; claim 23),

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values (0097; 0114; 0124; claim 23).

16. As per **claims 16 and 21**, Peterka et al discloses a method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key (fig. 1; 0080; 0082);

and for each encrypted section:

receiving a decryption key in respect of the encrypted section (0080; 0082);

decrypting and playing back the encrypted section using the decryption key (0033; 0080; 0082).

What Peterka et al does not explicitly teach is

destroying the decryption key after completing playback of the encrypted section.

Stirling et al discloses a method comprising:

destroying the decryption key after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying the decryption key after completing playback of the encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

17. As per **claim 17**, Peterka et al failed to explicitly disclose the method, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

Stirling et al discloses a method comprising destroying decrypted data content at the customer processing platform after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

18. As per **claim 18**, Peterka et al discloses the method, wherein the communications medium is the public Internet (fig. 1).

19. As per **claim 19**, Peterka et al further discloses the method, wherein, for each encrypted section, the encryption key is the same as the decryption key (0080; 0082; 0117).

22. As per **claim 22**, Peterka et al further discloses the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform (0038; 0097; 0114; 0124).

23. As per **claim 23**, Peterka et al further discloses the method, wherein receiving

each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the decryption key from the transmission value (0097; 0114; 0124; claim 23).

39. As per **claim 39**, Peterka et al further discloses the system, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform (fig. 1);

means for receiving the plurality of encrypted sections (0080; 0082);

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section (0080; 0082);

means for decrypting and playing back the encrypted section using the decryption key (0080; 0082).

What Peterka et al does not explicitly teach is

means for destroying the decryption key, after completing playback of the encrypted section.

Stirling et al discloses means for destroying the decryption key, after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying decrypted data content at the customer processing platform after

completing playback of the encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

40. As per **claim 40**, Peterka et al discloses a data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content (figs. 1, 3, 8, 9 and 15); and

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys (fig. 1; 0080; 0082).

What peterka et al does not explicitly teach is permission request.

Stirling et al discloses permission request (0047).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the

method of permission request in view of the teachings of Stirling et al in order to ensure that content is used by only authorized users.

41. As per **claim 41**, Peterka et al further discloses the system, comprising a data network connecting the data content server and the data content download controller (fig. 1).

42. As per **claim 42**, Peterka et al further discloses the system, further comprising a plurality of data content download controllers connected to the data network (fig. 1).

Claims 14, and 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

14. As per **claims 14 and 33**, Peterka et al discloses the method, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous

possession of at most a subset of the plurality of decryption keys at any time (0080; 0082; 0117).

What Peterka et al does not explicitly teach is delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform.

Ginter et al discloses delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

Claims 20 and 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Stirling et al U.S. patent Application Publication No. 2003/0223583 A1 as applied to claim 16 above, and further in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

20. As per **claims 20 and 43**, both Peterka et al and Stirling et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data

content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform.

Ginter et al discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Negawa U.S. Patent Application Publication No. 2003/0046539 A1.

34. As per **claim 34**, Peterka et al further discloses a method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device (0072; 0123; 0145);

comparing the customer verification information with corresponding stored customer information (0145); and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer (figs. 8 and 9);

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content (fig. 5; 0145); and

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data (fig. 9; 0080; 0082).

What Peterka et al does not explicitly teach is

causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device.

Negawa discloses a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device (0078).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device in view of the teachings of Negawa et al in order to ensure that content is only used for the number of times permitted.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The reference cited to Medvinsky U.S. Patent Application Publication No. 2004/0114762 A1 is a document considered relevant to the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington D.C. 20231

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Hand delivered responses should be brought to the United States Patent and Trademark Office Customer Service Window:

Randolph Building,

401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
October 31, 2006

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600